

What is claimed is:

1 1. An authentication system, comprising:
2 a filter to monitor sessions between a client and a server
3 for proper authentication;
4 a plug-in coupled to the client and the server, said plug-in
5 to generate public and private key pairs, and to receive and
6 store certificates; and
7 an extension coupled to said filter, said extension to
8 generate script commands to cause the client and the server to
9 perform required operations indicated by said filter.

10 2. The system of claim 1, wherein the certificates are
11 used to certify the client to the server.

12 3. The system of claim 1, wherein the certificates are
13 used to certify the server to the client.

14 4. The system of claim 1, wherein the certificates are
15 used to certify the client and the server to each other.

16 5. The system of claim 1, wherein the script commands are
17 implemented in a hypertext markup language (HTML) program.

1 6. A secure client/server system, comprising:

2 a client to request data or service;

3 a server to provide the requested data or service; and

4 an authentication system including:

5 a filter to monitor sessions between the client and the
6 server for proper authentication,

7 a plug-in coupled to the client and the server, said
8 plug-in to generate public and private key pairs, and to receive
9 and store certificates, and

10 an extension coupled to said filter, said extension to
11 generate script commands to cause the client and the server to
12 perform required steps indicated by said filter.

13 7. The system of claim 6, wherein the certificates are
14 used to certify the client to the server.

15 8. A method for providing a single sign-on authentication
16 and privacy, comprising:

17 submitting a request to access a node;

18 directing to submit a certificate;

19 verifying the submitted certificate with a trusted
20 certificate;

21 performing a challenge;

22 generating a response to the challenge; and

23 saving the response as a named cookie.

1 9. The method of claim 8, wherein said response is used as
2 a security token.

1 10. The method of claim 9, wherein said security token is
2 used to propagate an initial authentication.

1 11. The method of claim 8, further comprising:
2 creating a connection session if the certificate is valid.

1 12. The method of claim 8, wherein said verifying the
2 submitted certificate includes matching a signature on the
3 submitted certificate with a signature on the trusted
4 certificate.

1 13. The method of claim 8, further comprising:
2 generating a key;
3 encrypting the key with a client's public key;
4 sending an encrypted key to a client; and
5 using the encrypted key to encrypt communication.

1 14. A method for providing client privacy, comprising:
2 generating a key;
3 encrypting the key with a client's public key;
4 sending an encrypted key to a client; and
5 using the encrypted key to encrypt communication.

1 15. The method of claim 14, wherein said sending the
2 encrypted key includes sending the key using a hypertext transfer
3 protocol (HTTP) header.

1 16. A method for providing a single sign-on authentication
2 and privacy, comprising:
3 submitting a request to access a node;
4 directing to submit a certificate;
5 verifying the submitted certificate with a trusted
6 certificate;
7 performing a challenge;
8 generating a response to the challenge;
9 saving the response as a named cookie with an authentication
10 token; and
11 using standard Secure Socket Layer (SSL) library to provide
12 communication privacy.

1 17. The method of claim 16, wherein said verifying includes
2 creating and registering new authentication session.

1 18. The method of claim 17, wherein said verifying includes
2 validating the new authentication session with the authentication
3 token.

1 19. The method of claim 16, wherein said verifying includes
2 indicating a failure status to a client if said verifying fails.

1 20. The method of claim 16, wherein said performing said
2 challenge includes generating a node challenge random number.

1 21. The method of claim 16, wherein said directing includes
2 receiving an address of the node; and
3 checking to determine if the address is protected.

22. The method of claim 16, further comprising:
determining if the authentication token is already present.

23. The method of claim 22, further comprising:
determining if a client is on an access control list if the
authentication is present and valid.

1 24. An apparatus comprising a computer-readable storage
2 medium having executable instructions that enable the computer
3 to:

4 submit a request to access a node;
5 direct to submit a certificate;
6 verify the submitted certificate with a trusted certificate;
7 perform a challenge;
8 generate a response to the challenge; and
9 save the response as a named cookie.

10 25. The apparatus of claim 24, wherein said response is
11 used as a security token.

12 26. An apparatus comprising a computer-readable storage
13 medium having executable instructions that enable the computer
14 to:

15 submit a request to access a node;
16 direct to submit a certificate;
17 verify the submitted certificate with a trusted certificate;
18 perform a challenge;
19 generate a response to the challenge;
20 save the response as a named cookie with an authentication
21 token; and
22 use standard Secure Socket Layer (SSL) library to provide
23 communication privacy.

10559/214001/ P8707

1

2

3

1

THE UNIVERSITY OF CHICAGO